(19) BUNDESREPUBLIK DEUTSCHLAND

DEUTSCHES PATENTAMT

(12) **Offenlegungsschrift**

(10) **DE 195 23 009 A 1**

(51) Int. Cl.[6]:
G 06 K 19/073
G 07 C 9/00
B 60 R 25/04
H 04 L 9/32
E 05 B 65/12
// E05B 49/00

(21) Aktenzeichen: 195 23 009.4
(22) Anmeldetag: 24. 6. 95
(43) Offenlegungstag: 9. 1. 97

DE 195 23 009 A1

(71) Anmelder:
f + g megamos Sicherheitselektronik GmbH, 51674 Wiehl, DE

(74) Vertreter:
Cohausz & Florack, 40472 Düsseldorf

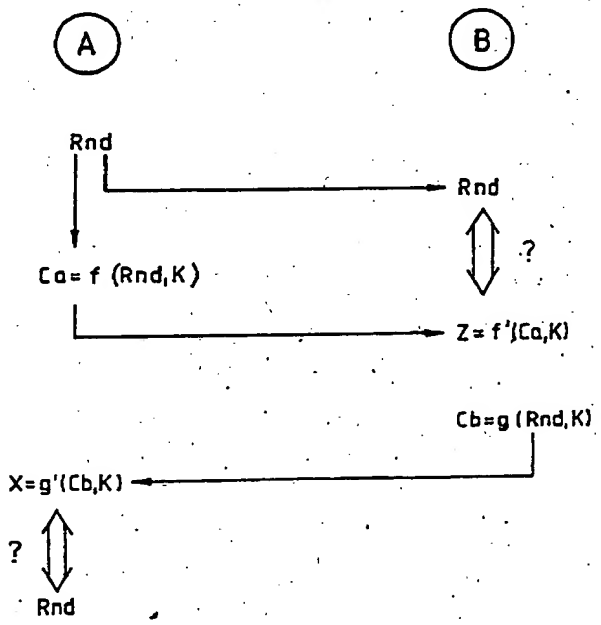
(72) Erfinder:
Konrad, Reimund, Dipl.-Ing., 51647 Gummersbach, DE; Spreng, Markus, Dipl.-Ing., 51588 Nümbrecht, DE

(56) Entgegenhaltungen:
DE 34 26 006 A1

Prüfungsantrag gem. § 44 PatG ist gestellt

(54) Authentifizierungssystem

(57) Die Erfindung betrifft ein Verfahren zur Prüfung der Nutzungsberechtigung für Zugangskontrolleinrichtungen, insbesondere Schließeinrichtungen für Fahrzeuge, bei dem zwischen einer dauerenergieversorgten zugangsseitigen Steuereinrichtung (A) und einer benutzerseitigen Schlüsseleinrichtung (B) nach einem geheimen Schlüssel (K) codierte Benutzercodeinformationen bidirektional ausgetauscht werden, wobei zur Feststellung der für die Freigabe der Zugangseinrichtung erforderlichen Berechtigung eine lokal erzeugte Zahlenfolge mit einer nach einer Verschlüsselung der Zahlenfolge auf die Gegenseite übertragenen, dort invers verschlüsselten und zurückübertragenen Information verglichen wird. Zur Verbesserung der Sicherheit des Verfahrens gegen Manipulation ist vorgesehen, daß zunächst die in der Steuereinrichtung (A) erzeugte und von dort zur Schlüsseleinrichtung (B) übertragene unverschlüsselte Zahlenfolge Rnd mit der in der Schlüsseleinrichtung (B) invers verschlüsselten von der Steuereinrichtung (A) gesendeten verschlüsselten Information Ca verglichen wird und daß bei Feststellung einer mangelnden Übereinstimmung die Berechtigungsprüfung abgebrochen wird.



DE 195 23 009 A1

Beschreibung

Die Erfindung betrifft ein Verfahren und eine Vorrichtung zur Prüfung der Nutzungsberechtigung für Zugangskontrolleinrichtungen insbesondere Schließeinrichtungen für Fahrzeuge, bei dem zwischen einer dauerenergieversorgten zugangsseitigen Steuereinrichtung und einer benutzerseitigen Schlüsseleinrichtung nach einem geheimen Schlüssel codierte Benutzercodeinformationen bidirektional ausgetauscht werden, wobei zur Feststellung der für die Freigabe der Zugangseinrichtung erforderlichen Berechtigung eine lokal erzeugte Zahlenfolge mit einer nach einer Verschlüsselung der Zahlenfolge auf die Gegenseite übertragenen, dort invers verschlüsselten und zurückübertragenen Information verglichen wird.

Ein Verfahren bzw. eine Vorrichtung dieser Art kommt immer dann zum Einsatz, wenn es um die Überprüfung geht, ob eine bestimmte Person authorisiert ist, die Zugangskontrolleinrichtung zu passieren. Dies gilt sowohl für ortsfeste Zugangskontrolleinrichtungen, zu denen nur ein ausgewählter Personenkreis zutritt hat. Dies gilt aber auch für mobile Zugangseinrichtungen, insbesondere an Fahrzeugen wie Kraftfahrzeugen, Schiffen oder Fahrrädern. Durch das Vorsehen von Zugangskontrolleinrichtungen soll hier dem Diebstahl des Fahrzeugs entgegengewirkt werden. Die Vorrichtung setzt sich dabei zusammen aus den beiden Grundkomponenten, zum einen der innerhalb der Zugangskontrolleinrichtung angeordneten Steuereinrichtung, welche dauerhaft mit Energie versorgt ist, und zum anderen der mobilen Schlüsseleinrichtung, die den authorisierten Benutzer identifizieren soll. Die Schlüsseleinrichtung kann dabei selbst Teil eines Fahrzeugschlüssels sein, welcher mit der Steuereinrichtung im Bereich der Schließanlage des Fahrzeuges in bidirektionalem Datenaustausch steht. Es kann sich aber auch um eine Chipkarte handeln, mittels der der Datenaustausch mit der Steuereinrichtung galvanisch gekoppelt erfolgt.

Verfahren bzw. Vorrichtungen zur Prüfung der Nutzungsberechtigung sind aus der Praxis im Anwendungsbereich für Fahrzeuge bekannt. Im einfachsten Fall handelt es sich um ein elektromagnetisches Identifizierungssystem bestehend aus einem im Zündschlüssel integrierten passiven Datenträger in Form eines Transponders, sowie einer am Zündschloß angebrachten Antennenspule, die mit der Steuereinrichtung verbunden ist. Ein solches System wird in der Regel über den Zündkontakt des Fahrzeuges aktiviert, wodurch das Steuergerät ein magnetisches Wechselfeld aussendet. Dieses regt den Datenträger im Transponder zum Aussenden seiner festabgespeicherten Dateninformation an. Die vom Steuergerät empfangenen Daten werden wiederum demoduliert und in der Steuereinrichtung mit einer in einer Schüsseltabelle abgelegten Vorgabeinformation verglichen. Nur im Falle einer Übereinstimmung kann das Fahrzeug gestartet werden.

Eine weitere Vorrichtung bzw. Verfahren zur Prüfung der Nutzungsberechtigung für Fahrzeuge ist das aus der Praxis ebenfalls bekannte sogenannte "challenge and response Verfahren". Hierbei sendet die Steuereinrichtung zunächst an die Schlüsseleinrichtung eine beliebige Dateninformation. Diese wird in der Schlüsseleinrichtung mit einem geheimen Schlüssel unter Verwendung einer Verschlüsselungsfunktion verschlüsselt. Die verschlüsselte Information wird an die Steuereinrichtung zurückgesendet. Die Steuereinrichtung wendet nun auf die empfangene Nachricht die Inversfunktion zur Verschlüsselungsfunktion in Verbindung mit dem geheimen Schlüssel an. Die dadurch erzeugte Information wird in der Steuereinrichtung verglichen mit der ursprünglich erzeugten Ausgangsfunktion. Wenn eine Übereinstimmung vorliegt, wird die Nutzungsberechtigung als gegeben angesehen. Ein Nachteil dieses Verfahrens ist darin zu sehen, daß die an sich geheime Verschlüsselungsfunktion der Schlüsseleinrichtung dadurch festgestellt werden kann, daß die Schlüsseleinrichtung von einem entsprechenden Manipulationsgerät häufig mit einer beliebigen Zahlenfolge angeregt wird und die von der Schlüsseleinrichtung erzeugte Information erfaßt und aufgezeichnet wird. Durch das mehrmalige zyklische Erzeugen von Zufallsnachrichten kann sowohl der geheime Schlüssel der Schlüsseleinrichtung als auch die Verschlüsselungsfunktion ermittelt werden. Eine Verbesserung der Sicherheit einer solchen Vorrichtung bzw. eines solchen Verfahrens ist nur graduell dadurch möglich, daß eine Verschlüsselungsfunktion bzw. ein geheimer Schlüssel mit einer sehr langen Zahlenfolge verwendet werden. Dies erhöht jedoch den erforderlichen Aufwand beträchtlich.

Neben diesem aus der Praxis bekannten Stand der Technik sind aus der DE 32 34 539 A1 bzw. der DE 33 13 098 C1 Vorrichtungen bzw. Verfahren zur Prüfung der Nutzungsberechtigung für Fahrzeuge bekannt, bei denen schlüsselseitig bzw. fahrzeugseitig nach jeder erfolgreichen Durchführung der Nutzungsberechtigungsprüfung jeweils eine neue, zufällig ausgewählte oder deterministisch festgelegte berechtigende Codeinformation für die nachfolgende Prüfung erzeugt wird.

Aus der DE 32 25 754 A1 ist ein Verfahren zur Prüfung der Nutzungsberechtigung für Schließanlagen bekannt, bei welchem auf einen schlüsselseitig ausgelösten Startimpuls hin zunächst Zufallszahlen generiert und zu Schloß- bzw. Schlüsselseite hin übermittelt werden, anschließend schlüssel- und schloßseitig unabhängig voneinander mit beidseitig übereinstimmenden Zufallszahlen jeweils entsprechende Rechenoperationen ausgeführt werden und jeweils ein bestimmtes Teilstück des Resultats der Rechenoperation auf die Gegenseite übertragen wird, mit dem entsprechenden Teilstück des dort vorliegenden Resultats verglichen und im Fall der Übereinstimmung ein Freigabeimpuls abgegeben wird.

Der Erfindung liegt davon ausgehend die Aufgabe zugrunde, eine Vorrichtung bzw. ein Verfahren der eingangs genannten Art dahingehend zu verbessern, daß bei vertretbarem elektronischen Aufwand die Sicherheit der Nutzungsberechtigungsprüfung verbessert wird.

Diese Aufgabe wird erfindungsgemäß bei dem Verfahren der eingangs genannten Art dadurch gelöst, daß zunächst die in der Steuereinrichtung erzeugte und von dort zur Schlüsseleinrichtung übertragene unverschlüsselte Zahlenfolge Rnd mit der in der Schlüsseleinrichtung invers verschlüsselten von der Steuereinrichtung gesendeten verschlüsselten Information Ca verglichen wird und daß bei Feststellung einer mangelnden Übereinstimmung die Berechtigungsprüfung abgebrochen wird.

Bei der Vorrichtung der eingangs genannten Art wird diese Aufgabe dadurch gelöst, daß die Schlüsseleinrichtung (B) von der Steuereinrichtung (A) sowohl die unverschlüsselte Zahlenfolge Rnd als auch eine verschlüsselte Information Ca empfängt und daß in der Schlüsseleinrichtung (B) weitere Mittel vorgesehen sind zum Vergleich der Zahlenfolge Rnd mit der in der Schlüsseleinrichtung (B) invers verschlüsselten Information der-

art, daß bei der Feststellung einer mangelnden Übereinstimmung die Berechtigungsprüfung abgebrochen wird.

Die Erfindung zeichnet sich dadurch aus, daß die Manipulationsmöglichkeiten an der Schlüsseleinrichtung unterbunden, jedenfalls aber ganz erheblich erschwert werden. Im Gegensatz zu den aus dem Stand der Technik bekannten Lösungen, bei denen der Schlüssel jeweils auf ein beliebiges von außen auf ihn einwirkendes Dateninformationssignal durch Aussenden einer entsprechenden Verschlüsselungsinformation reagiert, wird durch die erfindungsgemäße Lösung erreicht, daß schlüsselseitig nur dann überhaupt eine Information abgegeben wird, wenn die Überprüfung in der Schlüsseleinrichtung ergeben hat, daß die unverschlüsselte Zahlenfolge Rnd gleich ist mit der in der Schlüsseleinrichtung invers verschlüsselten von der Steuereinrichtung gesendeten verschlüsselten Information. Die Schlüsseleinrichtung muß also zwei miteinander korrespondierende Informationen unabhängig voneinander empfangen, damit eine weitere Reaktion erfolgen kann. Nur unter der Bedingung, daß die Zufallszahlenfolge mit der in der Schlüsseleinrichtung niedergelegten Verschlüsselungsfunktion codiert worden ist, wird im Schlüssel ein Signal zurückgewonnen, welches identisch ist mit der ursprünglichen Zufallszahlenfolge. Ein Unberechtigter, der mit einer beliebigen Zufallszahlenfolge auf die Schlüsseleinrichtung einwirken will, kann keine Reaktion hervorrufen, da er die Verschlüsselungsfunktion der Steuereinrichtung nicht kennt und diese auch durch Manipulation derselben nicht ermitteln kann. Erst wenn die Prüfung innerhalb der Schlüsseleinrichtung das Ergebnis hervorgebracht hat, daß eine Übereinstimmung vorliegt, schließt sich der eigentliche Nutzungsberechtigungsprüfungsvorgang nach dem an sich bekannten "challenge and response Verfahren" an. Hierzu wird schlüsselseitig eine kodierte Dateninformation ausgegeben, diese mit der hierzu inversen Verschlüsselungsfunktion in der Steuereinrichtung dekodiert und mit der ursprünglichen Zufallszahlenfolge verglichen. Wenn diesbezüglich eine Übereinstimmung vorliegt, erfolgt die Freigabe der Zugangskontrolleinrichtung. Die erfindungsgemäße Lösung zeichnet sich also dadurch aus, daß dem von der Schlüsseleinrichtung aus imitiertem "challenge and response Verfahren" eine zusätzliche Prüfung vorgeschaltet ist, so daß die Schlüsseleinrichtung selbst gegen Manipulationen geschützt ist.

Bevorzugte Ausführungsformen der Erfindung gehen aus den Unteransprüchen hervor.

Die Erfindung wird im folgenden anhand eines Ausführungsbeispiels in Verbindung mit der Skizze nach der Figur näher erläutert:

Das System zur Prüfung der Nutzungsberechtigung ist gemäß Ausführungsbeispiel für den Einsatz in einer Wegfahrsperre für Kraftfahrzeuge ausgelegt. Die Vorrichtung besteht aus der im Bereich des Kraftfahrzeuges angeordneten Steuereinrichtung A und der im des Zündschlüssel vorgesehenen Schlüsseleinrichtung B.

Zu Beginn der Nutzungsberechtigungsprüfung wird in der ständig von der Autobatterie versorgten Steuereinrichtung A eine Zufallszahlenfolge Rnd generiert. Diese wird unverschlüsselt auf die Schlüsseleinrichtung B übertragen. Anschließend wird unter Anwendung des in der Steuereinrichtung A hinterlegten geheimen Codes K sowie der in der Steuereinrichtung abgespeicherten Verschlüsselungsfunktion f eine verschlüsselte Information Ca erzeugt, die ebenfalls zur Schlüsseleinrichtung B übertragen wird. Innerhalb der Schlüsseleinrichtung B wird nun auf die empfangene Information Ca die inverse Verschlüsselungsfunktion f' angewendet, die in der Schlüsseleinrichtung B hinterlegt ist, wiederum unter Benutzung des auch in der Schlüsseleinrichtung B hinterlegten geheimen Schlüssels K.

Anschließend werden beide Nachrichten miteinander verglichen, nämlich die Zufallszahlenfolge Rnd im nicht verschlüsselten Zustand sowie die inverse verschlüsselte Information Z.

Liegt eine Übereinstimmung beider Nachrichten vor, ist gewährleistet, daß eine Berechtigung vorliegt, da nur dann die inverse Information mit der ursprünglichen unkodierten Zufallszahlenfolge Rnd übereinstimmt, wenn diese zuvor in der Steuereinrichtung A mit der Verschlüsselungsfunktion f kodiert wurde.

Im Falle einer Abweichung beider Nachrichten, wird die Verschlüsselungseinrichtung in ihren Grundzustand zurückgesetzt, ohne daß Informationen gesendet werden. Hierdurch wird der Prüfungsvorgang abgebrochen, ohne daß der unberechtigte die Möglichkeit an weiteren Manipulationen an der Schlüsseleinrichtung erhält.

Falls eine Übereinstimmung der miteinander verglichenen Nachrichten vorliegt, wendet die Schlüsseleinrichtung B auf die Zufallszahlenfolge Rnd unter Berücksichtigung des geheimen Codes K die weitere Verschlüsselungsfunktion g an, die ebenfalls in der Verschlüsselungseinrichtung B abgespeichert ist. Diese mit Cb bezeichnete Information wird im folgendem an die Steuereinrichtung A übermittelt, welche hierauf die inverse Verschlüsselungsfunktion g' in Verbindung mit dem geheimen Schlüssel K anwendet.

Wenn dann die hieraus gewonnene Nachricht X wiederum der ursprünglichen Zufallszahlenfolge Rnd entspricht, ist die Nutzungsberechtigung nachgewiesen, so daß die entsprechende Fahrzeugkomponente freigegeben werden.

In weiteren, nicht dargestellten Ausführungsbeispielen läßt sich das erfindungsgemäße Verfahren bzw. die erfindungsgemäße Vorrichtung auch auf andere Arten von Zugangskontrolleinrichtungen anwenden, beispielsweise sogenannte Keylessentry-Systeme, bei denen anstelle eines Schlüssels eine Codekarte verwendet wird.

Patentansprüche

1. Verfahren zur Prüfung der Nutzungsberechtigung für Zugangskontrolleinrichtungen, insbesondere Schließeinrichtungen für Fahrzeuge, bei dem zwischen einer dauerenergieversorgten zugangsseitigen Steuereinrichtung (A) und einer benutzerseitigen Schlüsseleinrichtung (B) nach einem geheimen Schlüssel (K) codierte Benutzercodeinformationen bidirektional ausgetauscht werden, wobei zur Feststellung der für die Freigabe der Zugangseinrichtung erforderlichen Berechtigung eine lokal erzeugte Zahlenfolge mit einer nach einer Verschlüsselung der Zahlenfolge auf die Gegenseite übertragenen, dort invers verschlüsselten und zurückübertragenen Information verglichen wird, **dadurch gekennzeichnet,** daß zunächst die in der Steuereinrichtung (A) erzeugte und von dort zur Schlüsseleinrichtung (B) übertragene unverschlüsselte Zahlenfolge Rnd mit der in der Schlüsseleinrichtung (B) invers verschlüsselten von der Steuereinrichtung (A) gesendeten verschlüsselten Information Ca verglichen wird und daß bei Feststellung einer mangelnden Übereinstimmung die Berechtigungsprüfung abgebrochen wird.

2. Verfahren nach Anspruch 1, gekennzeichnet

durch die Merkmale:

a) in der Steuereinrichtung (A) wird eine Zufallszahlenfolge Rnd erzeugt;

b) die Zufallszahlenfolge Rnd wird zur Schlüsseleinrichtung (B) übertragen;

c) die Zufallszahlenfolge wird in der Steuereinrichtung (A) mittels einer ersten Verschlüsselungsfunktion f codiert;

d) die mittels der ersten Verschlüsselungsfunktion f codierte Information Ca wird zur Schlüsseleinrichtung (B) übertragen;

e) die mittels der ersten Verschlüsselungsfunktion f codierte Information Ca wird in der Schlüsseleinrichtung (B) mittels einer ersten inversen Verschlüsselungsfunktion f' entschlüsselt;

f) die mittels der ersten inversen Verschlüsselungsfunktion f' entschlüsselte Information Z wird in der Schlüsseleinheit (B) mit der Zufallszahlenfolge Rnd verglichen;

g) im Falle einer festgestellten Übereinstimmung der mittels der ersten inversen Verschlüsselungsfunkktion f' entschlüsselten Information Z mit der Zufallszahlenfolge Rnd wird in der Schlüsseleinheit (B) die Zufallszahlenfolge Rnd mit einer zweiten Verschlüsselungsfunktion g verschlüsselt;

h) die mit der zweiten Verschlüsselungsfunktion g verschlüsselte Information Cb wird zur Steuereinrichtung (A) übertragen;

i) die mit der zweiten Verschlüsselungsfunktion g verschlüsselte Information Cb wird in der Steuereinrichtung (A) mittels einer zweiten inversen Verschlüsselungsfunktion g' entschlüsselt;

j) die mittels der zweiten inversen Verschlüsselungsfunktion g' entschlüsselte Information X wird in der Steuereinrichtung (A) mit der Zufallszahlenfolge Rnd verglichen;

k) bei einer Übereinstimmung der mittels der zweiten inversen Verschlüsselungsfunktion g' entschlüsselten Information X mit der Zufallszahlenfolge Rnd erfolgt eine Freigabe der Zugangskontrolleinrichtung.

3. Verfahren nach einem der vorhergehenden Ansprüche dadurch gekennzeichnet, daß in Steuereinrichtung (A) und Schlüsseleinrichtung (B) unterschiedliche geheime Schlüssel (Ka, Kb) verwendet werden.

4. Vorrichtung zur Prüfung der Benutzerberechtigung für Zugangskontrolleinrichtungen, insbesondere Schließeinrichtungen für Fahrzeuge, mit einer dauerenergieversorgten zugangsseitigen Steuereinrichtung (A) und einer benutzerseitigen Schlüsseleinrichtung (B), zwischen denen nach einem geheimen Schlüssel (K) codierte Benutzercodeinformationen über Sende- bzw. Empfangsmittel bidirektional austauschbar sind, wobei zur Feststellung der für die Freigabe der Zugangseinrichtung erforderlichen Berechtigung Mittel vorgesehen sind zum Vergleich einer lokal erzeugten Zahlenfolge mit einer nach einer Verschlüsselung der Zahlenfolge auf die Gegenseite übertragenen, dort invers verschlüsselten und zurückübertragenen Information, dadurch gekennzeichnet, daß die Schlüsseleinrichtung (B) von der Steuereinrichtung (A) sowohl die unverschlüsselte Zahlenfolge Rnd als auch eine verschlüsselte Information Ca empfängt und daß in der Schlüsseleinrichtung (B) weitere Mittel vorgesehen sind zum Vergleich der Zahlenfolge Rnd mit der in der Schlüsseleinrichtung (B) invers verschlüsselten Information derart, daß bei der Feststellung einer mangelnden Übereinstimmung die Berechtigungsprüfung abgebrochen wird.

5. Vorrichtung nach Anspruch 4, gekennzeichnet durch

— einen Zufallszahlengerator in der Steuereinrichtung (A) zur Erzeugung einer Zufallszahlenfolge Rnd;

— eine erste, in der Steuereinrichtung (A) angeordnete Verschlüsselungseinrichtung mit einer ersten Verschlüsselungsfunktion f zur Verschlüsselung der Zufallszahlenfolge Rnd zu einer Information Ca;

— eine erste, in der Schlüsseleinrichtung (B) angeordnete Entschlüsselungseinrichtung mit einer zur ersten Verschlüsselungsfunktion inversen Verschlüsselungsfunktion zur Erzeugung einer Information Z;

— eine erste, in der Schlüsseleinrichtung angeordnete Vergleichereinrichtung zum Vergleich der Zufallszahlenfolge Rnd mit der nach der ersten Verschlüsselungsfunktion verschlüsselten und mittels der inversen Verschlüsselungsfunktion entschlüsselten Information Z;

— eine zweite, in der Schlüsseleinrichtung (B) angeordnete Verschlüsselungseinheit mit einer zweiten Verschlüsselungsfunktion g zur Verschlüsselung der Zufallszahlenfolge Rnd zu einer Information Cb;

— eine zweite, in der Steuereinrichtung (A) angeordnete Entschlüsselungseinrichtung mit einer zur zweiten Verschlüsselungsfunktion g inversen Verschlüsselungsfunktion g';

— eine zweite, in der Steuereinrichtung (A) angeordnete Vergleichereinrichtung zum Vergleich der Zufallszahlenfolge Rnd mit der nach der zweiten Verschlüsselungsfunktion g verschlüsselten und mittels der inversen Verschlüsselungsfunktion g' entschlüsselten Information X;

— Steuermittel zum Ansteuern der vorstehend genannten Komponenten derart, daß nur bei einer in der Schlüsseleinrichtung (B) mittels der ersten Vergleichereinrichtung festgestellten Übereinstimmung eine Übermittlung der mittels der zweiten Verschlüsselungsfunktion g verschlüsselten Zufallszahlenfolge Cb an die Steuereinrichtung (A) erfolgt.

6. Vorrichtung nach einem der Ansprüche 4 oder 5, dadurch gekennzeichnet, daß die Schlüsseleinrichtung (B) ein insbesondere als Transponder ausgebildeter Teil eines Fahrzeugschlüssels ist.

7. Vorrichtung nach einem der Ansprüche 4 oder 5, dadurch gekennzeichnet, daß die Kopplung zwischen Steuereinrichtung (A) und Schlüsseleinrichtung (B) galvanisch, insbesondere in Form einer Chipkarte, erfolgt.

8. Vorrichtung nach einem der Ansprüche 4 oder 5, dadurch gekennzeichnet, daß die Kopplung zwischen Steuereinrichtung (A) und Schlüsseleinrichtung (B) kapazitiv erfolgt.

Hierzu 1 Seite(n) Zeichnungen

– Leerseite –

Numm
Int. Cl.[6]: DE 195 23 009 A1
G 06 K 19/073
Offenlegungstag: 9. Januar 1997